DIGITAL SIGNATURES FOR TANGIBLE MEDIUM

ABSTRACT

The invention provides a method for a sender to send a message on a tangible medium and ensure that it is privacy protected until verification that the medium has been received by the authorized recipient. The invention provides a method in which a sender creates an encrypted content message that may be decrypted using a content decryption key that is unknown to the authorized recipient. The sender creates an encrypted authentication message that may be decrypted using a recipient's key that is known to the authorized recipient but is unknown to others, except perhaps to the sender. The sender fixes the encrypted content message and the encrypted authentication message onto a tangible medium and then permits the authorized recipient to obtain the tangible medium. The authorized recipient uses the recipient's key to decrypt the encrypted authentication message and then creates a valid reply that is based upon or which uses the decrypted authentication message. The authorized recipient sends the valid reply to the sender and upon verification that the reply is valid the sender allows the authorized recipient to obtain the content decryption key. With the content decryption key, the authorized recipient is able to decrypt the encrypted content message. The invention also includes an article of manufacture for sending an encrypted message from a sender to an authorized recipient using a method of the invention.